

## ABSTRACT OF THE DISCLOSURE

A method of cryptographic encryption and decryption by a recipient selecting a modulus  $p$  from  $p=(2^{dk}-2^{ck}-1)/r$ ;  $p=(2^{dk}-2^{(d-1)k}+2^{(d-2)k}-\dots-2^k+1)/r$ ;  $p=(2^{dk}-2^{ck}-1)/r$ ;  $p=(2^{dk}-2^{ck}+1)/r$ ; and  $p=(2^{4k}-2^{3k}+2^{2k}+1)/r$ ; the recipient selecting a curve  $E$  and an order  $q$ ; the recipient selecting a base point  $G=(G_x, G_y)$  on the elliptic curve  $E$ ; the recipient generating a private integer  $w$ ; the recipient generating a public key  $W$ , where  $W=wG$ ; the recipient distributing  $p$ ,  $E$ ,  $q$ ,  $G$ , and  $W$  in an authentic manner; a sender retrieving the recipient's public key  $W$ ; the sender generating a private integer  $r$ ; the sender generating  $R=rG$  using the form of recipient's modulus  $p$ , and where  $G$  is recipient's basepoint; the sender combining  $r$ ,  $W$ , and  $M$  using the form of recipient's modulus  $p$  to form ciphertext  $C$ ; the sender sending  $(R, C)$  to the recipient; the recipient retrieving its private key  $w$ ; the recipient receiving  $(R, C)$ ; and the recipient combining  $R$ ,  $w$ , and  $C$  using the form of recipient's modulus  $p$  to recover  $M$ .

09926703-080901  
T96080-00492660